Study of Single Family Property Management Systems and Data

System Security and Privacy Plan

June 16, 2003

Office of Housing

Federal Housing Administration

Department of Housing and Urban Development

System Security and Privacy Plan

Table of Contents

1.0 GENERAL INFORMATION

1.0 GENERAL INFORMATION

The Federal Housing Administration's (FHA's) Office of Insured Single Family Housing administers a property management program and oversees the acquisition, marketing, and disposition of approximately 60,000 properties per year. Single Family Housing maintains the Single Family Acquired Asset Management System (SAMS) and other property management support systems to assist with program operations, such as case management, financial management, contractor monitoring, business evaluation, and business partner management. SAMS and the other systems must fully support these business functions in order for FHA to effectively and efficiently manage its program.

Since the original implementation of SAMS, Single Family Housing has changed the property management program and its business model. In an effort to streamline operations, FHA began contracting out the Real Estate Owned (REO) functions in 1997. Consequently, Single Family Housing's role shifted to oversight and monitoring rather than performing the day-to-day REO activities. Over time, FHA adapted SAMS and developed supplemental systems to support both the property management and contractor oversight functions. While FHA has made extensive modifications to SAMS and developed other support systems, numerous challenges remain with its property management operations within the current systems environment. For example, maintenance costs remain excessively high. Furthermore, FHA has received criticisms from the General Accounting Office (GAO) about its single-family property management operations, systems, and monitoring performance in various studies. As a result, GAO has placed Single Family on its high-risk list since 1994. In its financial statements, FHA also has received material weaknesses and reportable conditions related to single-family systems, including:

- FHA's systems environment provides insufficient support to its business processes.
- FHA lacks control over budget execution and funds.
- FHA performs inadequate monitoring over its Single Family property inventory.

1.1 Purpose

Single Family Housing seeks to increase SAMS' functionality or implement a new system. FHA needs to assess its long-term business needs and the capacity of its current systems prior to any further systems development efforts. The development of *The System Security and Privacy Plan* supports the assessment and planning process. This document provides an overview of the security requirements of the proposed property management system and the controls in place or being planned for meeting those requirements. This document addresses information sensitivity, levels of security, security risks, and control measures.

SAMS is identified as a Major Application in accordance with National Institute of Standards and Technology (NIST) *Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems*. Given the importance of this application to FHA's mission, FHA recognizes adequate security of information and the proposed system that processes the data is a fundamental management responsibility. FHA understands the need for an information security program and controls to make informed judgments and investments to mitigate risks to acceptable levels. As a result, FHA has begun to develop its *System Security and Privacy Plan* during the Initiate Phase – rather than Define Phase – of the System Development Methodology (SDM).

FHA recognizes that some sections of this document such as personnel security, physical and environmental protection, production and input/output controls, contingency planning, application software maintenance controls, data validation controls, training, identification and authentication require further development. FHA will continue to refine the *Security and Privacy Plan* throughout the phases of HUD's SDM. In addition, FHA may choose to review and update the plan whenever any of the following occur:

- Significant changes in program scope, business processes, system design and architecture.
- Application improvements and upgrades.
- Modifications in tools and techniques used for security controls.

The Federal Information Technology Security Assessment Framework provides a tool for guiding the routine assessment of security programs and prioritizing efforts for improvement. The framework is divided into five levels:

- Level 1 – Control objectives documented in a security policy.
- Level 2 – Security controls documented as procedures.
- Level 3 – Implemented procedures and controls.
- Level 4 – Tested and reviewed procedures and controls.
- Level 5 – Fully integrated procedures and controls.

Each level represents a more complete and effective security program. FHA will take steps to bring the proposed property management system to the highest level of operations.

1.2 Scope

This project provides FHA with a blueprint for property management and helps guide FHA towards an improved way of conducting its business. FHA performed an in-depth review of the Single Family systems supporting the property management function, including asset management, business participant management, business evaluation, and financial management. Based on this analysis, we presented an alternative solution to its current systems environment. FHA conducted this study in five primary phases:

- Phase I – Identify major business and system needs.
- Phase II – Identify major deficiencies in the current systems.
- Phase III – Develop short- and long-term alternatives.
- Phase IV – Present findings and obtain stakeholder buy-in.
- Phase V – Develop Initiate phase documents, including the *Project Plan, Needs Assessment, Feasibility Study, Risk Analysis, Cost-Benefit Analysis, System Security Plan*, and *Systems Decision Paper*.

1.3 System Overview

While the Department of Housing and Urban Development's (HUD) Information Technology (IT) division provides technical assistance, HUD's Office of Housing is responsible for the

identification of business process and reporting needs of its systems. For single-family mortgage insurance programs, the Office of Single Family Programs and the Office of the Comptroller share responsibility for SAMS and other single-family systems.

SAMS is a mixed program and financial management system that accounts for the sale of over 60,000 properties valued at over $5 billion dollars and related expenses totaling nearly $1 billion per year. SAMS supports HUD staff at Headquarters, Homeownership Centers (HOCs), and Management and Marketing (M&M) contractors with tracking single-family properties from acquisition through resale. In addition to collecting data related to the management, marketing, and disposition of properties, SAMS maintains financial records in compliance with the Federal Credit Reform Act and processes disbursements to M&M contractors, vendors, taxing authorities, and homeowners' associations.

SAMS is hosted on HUD's IBM-compatible mainframe and is connected to HUD's network, HINET, through a COMTEN front-end processor. Software used in SAMS includes: COBOL, DB2, CICS, EXTRA, JCL, NOMAD, and the Configuration Management tool, Endevor. SAMS development tools include Electronic Data System's (EDS) proprietary case tool – INCASE.

The following table provides the requisite system information.

Responsible Organization	Federal Housing Administration – Office of Housing
System Name or Title	Single Family Acquired Asset Management System (SAMS)
System Code	A80S
Project Cost Accounting Sub-system (PCAS) Number	To Be Determined
System Category	Major application
Operational Status	Operational
Users	FHA and M&M contractors
System Input	Mortgagee data, transmittal check data, property acquisition data, claim data, lockbox and Fedwire collection data, check data, valid property case data, property maintenance data, property acquisitions
System Output	New acquisitions, inventory status and sales data, property listing, property title data, SAMS general ledger balances, disbursement data, and sales related data.
Interaction With Other Systems	The SAMS environment is composed of numerous interconnected and stand alone systems. SAMS shares data with the following systems through manual or automated interfaces: Single Family Insurance System (SFIS),

	Computerized Homes Underwriting Management System (CHUMS), Institutional Master File (IMF), A80N, Single Family Insurance Claims Subsystem, Lockbox, File Transfer Protocol (FTP) Server, HUD Web, Kiosks, Single Family Data Warehouse, TEAM, Fedwire system (Cashlink), Cash Control Accounting Reporting System (CCARS), ECS system (Electronic Funds Transfer (EFT) disbursements), and the FHA Subsidiary Ledger

1.4 Project References

FHA used the following reference materials to prepare the *System Security and Privacy Plan*.

Document	Date
EDS, HUD/SAMS Release Summary	No date noted
Information Technology Management Reform Act of 1996	No date noted
IBM Endowment for The Business of Government, *IT Outsourcing: A Primer for Public Managers,* Chen, Perry	February 2003
Joint Financial Management Improvement Program, *Property Management System Requirements*	October 2002
Management & Marketing Service Contract Terms and Conditions	No date noted
National Institute of Standards and Technology, *Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook*	October 1995
National Institute of Standards and Technology, *Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems*	September 1996
National Institute of Standards and Technology, *Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model (supersedes NIST Spec. Pub. 500-172)*	April 1998
National Institute of Standards and Technology, *Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems*	December 1998
National Institute of Standards and Technology, *Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems*	November 2001

Document	Date
National Institute of Standards and Technology, *Special Publication 800-40, Procedures for Handling Security Patches*	August 2002
National Institute of Standards and Technology, *Special Publication 800-44, Guidelines on Securing Public Web Servers*	September 2002
Office of Management and Budget Circular Number, A-130, *Management of Federal Information Resources, Appendix III*	November 2000
United States Department of Housing and Urban Development, *Business Process Reengineering*	March 1997
United States Department of Housing and Urban Development, *FHA Audit of Financial Statements Fiscal Years 2002 and 2001*	January 2003
United States Department of Housing and Urban Development, *Final Draft SAMS User's Guide*	August 2002
United States Department of Housing and Urban Development, *Management Structure Design and Specifications in the M&M Contract Environment For Single Family Property Disposition*	January 1999
United States Department of Housing and Urban Development, *M&M Contractor Compliance Review, Risk-Based Targeting Model Web Tool Training*	August 2002
United States Department of Housing and Urban Development, *Office of the Single Family Housing Target Architecture Development*	September 2002
United States Department of Housing and Urban Development, *Processing Procedures and Internal Controls for M&M Contractors*	No date noted
United States Department of Housing and Urban Development, *SAMS Reports Training Manual*	May 2002
United States Department of Housing and Urban Development, *Single Family Housing Target Architecture*	August 2002
United States General Accounting Office, *Financial Management: Strategies to Address Improper Payments at HUD, Education, and Other Federal Agencies*	October 2002
United States General Accounting Office, *Information Technology: Leading Commercial Practices for Outsourcing of Services*	November 2001

Document	Date
United States General Accounting Office, Loan Origination and Foreclosed Property Management Processes	November 1999
United States General Accounting Office, *Single Family Housing: Current Information Systems Do Not Fully Support the Business Processes at HUD's Homeownership Centers*	October 2001
United States General Accounting Office, *Single Family Housing: Improvements Needed in HUD's Oversight of the Property Sale Process*	April 2002
United States General Accounting Office, *Single Family Housing: Stronger Measures Needed to Encourage Better Performance by Management and Marketing Contractors*	May 2002

1.5 Acronyms and Abbreviations

The following table lists the acronyms and abbreviations used in this document.

Acronym/Abbreviation	Definition
ADP	Automated Data Processing
ASP	Application Service Provider
CCARS	Cash Control Accounting Reporting System
CHUMS	Computerized Homes Underwriting System
CIO	Chief Information Officer
CO	Contracting Officer
EDS	Electronic Data Systems
EFT	Electronic Funds Transfer
FHA	Federal Housing Administration
FISMA	Federal Information Security Requirements Act
FTP	File Transfer Protocol
GAO	General Accounting Office

Acronym/Abbreviation	Definition
GTM	Government Technical Monitor
GTR	Government Technical Representative
HOC	Homeownership Center
HUD	U.S. Department of Housing and Urban Development
IDS	Intrusion Detection System
IMF	Institutional Master File
IT	Information Technology
M&M	Management and Marketing
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OCPO	Office of the Chief Procurement Officer
OIG	Office of Inspector General
OIT	Office of Information Technology
PCAS	Project Cost Accounting Sub-System
REO	Real Estate Owned
SAMS	Single Family Acquired Asset Management System
SDM	System Development Methodology
SFIS	Single Family Insurance System

1.6 Points of Contact

The following sections provide a listing of contacts for additional information regarding this document and the overall project, as well as a listing of departmental organizations and their contacts that provide support and guidance related to this project.

1.6.1 Information

This table provides a list of organizational points of contact that may be needed by the document user for informational and troubleshooting purposes. All contacts are located at 451 Seventh Street, SW, Washington, DC, 20410.

Type of Contact	Contact Name	Department	Telephone	Email/Address

1.6.2 Coordination

The following table provides a list of organizations that require coordination between the project and its specific support function. Intragency Memorandums of Understanding regarding data sharing, use, security and privacy are expected to be initiated and completed with these offices.

Type of Contact	Contact Name	Department	Telephone	Email/Address

Type of Contact	Contact Name	Department	Telephone	Email/Address

2.0 INFORMATION SENSITIVITY

2.0 INFORMATION SENSITIVITY

This section assesses the sensitivity of the information contained within the system and the risk level for confidentiality, integrity, and availability.

Property management information consists of data derived from multiple sources, such as appraisers, inspectors, and contractors. Some of the information is considered privacy data and may be sensitive to unauthorized access or release. The security of the databases, transmission, and analytics of its content must be evaluated and protected in accordance with the Privacy Act of 1974, HUD Privacy Handbook 1325.01 with revisions, and the Computer Matching and Privacy Protection Act of 1998. We also consider some personal identifying data, biometrics, disability information, personal financial information, debts, loans, income discrepancies, or investigations to potentially require additional security and privacy control considerations.

The sensitivity and criticality of the information stored within, processed by, or transmitted by a system provides a basis for the value of the system and is one of the major factors in risk management. It is important that FHA determine the sensitivity level of the information through an assessment of the requirements for availability, integrity, and confidentiality of the information.

2.1 Applicable Laws

There are numerous security and privacy related laws that will impact this application:

- *Office of Management and Budget (OMB) Circular A-127, Policies and Standards for Financial Management Systems*.
- *OMB Circular A-130, Management of Federal Information Resources*.
- Computer Security Act.
- Privacy Act.
- e-Government Act.
- Computer Matching and Privacy Protection Act.
- Patriot Act.

NIST provides security guidance useful to the development of security and privacy plans. Some recommended publications include:

- *Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook.*
- *Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems.*
- *Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model (supersedes NIST Spec. Pub. 500-172).*

- *Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems.*
- *Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.*
- *Special Publication 800-40, Procedures for Handling Security Patches.*
- *Special Publication 800-44, Guidelines on Securing Public Web Servers*.

In addition, HUD publishes guidance that must be followed:

- *HUD Handbook 2400.24, Rev. 2 ADP Security Program.*
- *HUD Handbook 1840.1, Departmental Management Control Program.*
- *HUD Handbook 2400.1, SDM Documentation Standards*
- *HUD Handbook 1325.01 with revisions, Privacy*.

2.2 Need for Protective Measures

FHA's Office of Insured Single Family Housing administers the property management program and oversees the acquisition, marketing, and disposition of approximately 60,000 properties per year. The proposed property management system will assist with program operations, such as asset management, financial management, business evaluation, and business partner management. As a result, the proposed system will contain confidential information, such as buyer social security numbers. It will also store property appraisal, bid, sales, and other financial information. Furthermore, financial information will be collected and transferred through a rules-based engine to FHA's subsidiary ledger for financial management, recordation, and funds control.

The need for HUD-established security policies are critical to realizing Single Family's mission, including physical security, non-disclosures, background checks, intrusion detection, counterfraud, anti-virus, and installation of firewalls. To comply with *OMB Circular A-127*, *Policies and Standards for Financial Management Systems*, FHA needs to identify security controls and incorporate these controls into operations in accordance with the *Computer Security Act* and *OMB Circular A-130, Management of Federal Information Resources, Appendix III* for those financial systems that contain sensitive information. Agencies must implement and maintain a security program to assure adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in major applications.

2.3 Sensitivity

Due to the type of information that will be contained in the proposed system, the confidentiality of the data and the integrity and availability of the system is critical. For example:

- FHA relies on the timely transmittal of claim information to the M&M contractor to initiate property preservation activities for newly acquired properties.

- M&M contractors and taxing authorities depend upon accurate and timely payment of fees and reimbursable expenses from FHA. The data needs to be protected from unanticipated or unintentional modification.
- The proposed property management system transmits financial information to FHA's Subsidiary Ledger, which produces the organization's financial statements.

FHA needs to consider several criteria to develop the ratings of the process sensitivity for the proposed property management system.

2.3.1 Integrity

Integrity is a measure of the overall accuracy of the data and the related process. Only authorized users are allowed to make modifications. Integrity includes, but is not limited to:

- Authenticity – The origin of a message must be correctly identified and the content of a message has not been changed in transit.
- Non-repudiation – The sender or receiver of a specific message cannot deny the transmission.
- Accountability – A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

FHA will base the required level of integrity on the impact of unauthorized creation, alteration, or destruction of data/process. Possible definitions for rating integrity are:

- Low – If integrity is compromised it will have a negligible or minimal impact on FHA's missions, functions, image, or reputation and will not require significant resources to correct.
- Medium – If integrity is compromised it may have a significant adverse impact to FHA's missions, functions, image, or reputation and may require significant resources to correct.
- High – If integrity is compromised it may have a severe impact, permanently violating the integrity of FHA's missions, functions, image, or reputation. It will result in the loss of major tangible assets(s), resource(s), or effect FHA's ability to conduct business operations causing loss, which is irreparable or requires excessive resources to correct.

2.3.2 Confidentiality

Confidentiality is a measure of the extent to which information must be protected from unauthorized disclosures during storage or transfer. This includes printing, displaying, revealing the existence of an object, or other forms of disclosure.

FHA will base the required level of confidentiality on the impact of data exposed to unauthorized view. Possible definitions for rating confidentiality are:

- Low – If data can be viewed by the public or will not cause a significant impact if viewed by the public.

- Medium – If data is viewed by the public or internal personnel it may have a significant impact (i.e., affect FHA's public relations) or if management believes data is sensitive to unauthorized viewing but will not jeopardize FHA's business operations.
- High – If data requires protection by policy or law (Privacy Act of 1974), or if confidentiality is compromised it may have a severe impact on FHA's business operations (e.g., affect law enforcement capabilities).

2.3.3 Availability

Availability is a measure of how long users could sustain their business functions without information, if necessary. FHA will base the level of availability required for the system on the impact of denied service to users and system administrators. Possible definitions for rating availability are:

- Low – If denial of service for more than one week will be unacceptable.
- Medium – If denial of service for more than a day will be unacceptable.
- High – If denial of service for more than a few hours will be unacceptable.

2.4 Security Risk

A quantifiable security risk assessment or security code review has not be performed to date. However, after reviewing the processes and information to be processed, we determined an interim risk rating for confidentiality, integrity and availability.

Rating Type	Rating Code	Description
Integrity	Medium	The accuracy of financial information is critical to the reputation of FHA and the timely processing of transactions. Data integrity is an important concern and considered to be medium sensitivity. Data must be protected from data intrusion, manipulation, loss, theft, and unwanted alteration. A compromise of the data integrity will have a significant adverse impact to the mission.

Rating Type	Rating Code	Description
Confidentiality	High	Personal data, including financial information not available by public means, requires protection by policy or law. Confidentiality is of high concern to avoid legal liabilities, a loss of public confidence, and penalties. The system contains private and financial information that requires protection from intrusion or unauthorized access, loss, damage, or release without consent, pre-arranged memorandum of understanding, or a need to know requirement. If compromised, this data will have a severe impact to FHA's business operations.
Availability	Medium	The system is heavily reliant on the Application Security Provider (ASP) and is subject to the availability of its supporting infrastructure and back-ups. The system contains information that needs to be processed in a timely manner to meet deadlines and to avoid losses. Outages extending 24 hours are unacceptable.

The major security risk for the application is the unauthorized access and disclosure of privacy or financial sensitive information. As such, the proposed solution will need to support data labeling and data classification. This concept, long practiced by military and national security systems, requires that information data fields or data families have labels such as unclassified, classified or top secret. Parallel to labeling data is the need for role-based access. Role-based access follows the concept that users are grouped by their job functions and receive only enough access to perform their job responsibilities. Together, the concepts of data labeling and role-based access will address concerns over unauthorized access and disclosure of privacy data. These risks will need to be mitigated once FHA selects the ASP. FHA will need to ensure that HUD-approved security processes, technologies, and tools are in place to provide adequate controls and protections for security and privacy.

Access controls, such as user ID and password protection, will help to mitigate unauthorized access with access levels commensurate with job responsibilities. Limiting system permissions reduces the risk that users will perform inappropriate functions. Other key protective measures, such as anti-virus, intrusion detection, and counterfraud programs, should exist within the system.

3.0 SYSTEM SECURITY MEASURES

3.0 SYSTEM SECURITY MEASURES

This section addresses the measures necessary for system security. The objective of system security planning is to improve protection of information technology resources. All federal systems have some level of sensitivity and require protection as part of good management practice. This plan describes the control measures intended to meet the protection requirements of the system as those control measures are developed. The types of control measures will be consistent with the need for protection of the system as described in *OMB Circular A-130, Management of Federal Information Resources, Appendix III*.

A comprehensive application security plan will be developed to identify the security requirements for the property management system. The application security plan will:

- Provide an overview of the security requirements for the system and describe the controls in place or planned for meeting those requirements.
- Delineate responsibilities and expected behavior of all individuals who access the system.

During the Define and Design phases of HUD's SDM, FHA will continue to refine this document. The *System Security and Privacy Plan* will be updated to identify new information, such as detailed security requirements for the proposed property management system and newly defined control measures.

3.1 Control Measures

This section outlines the management, operational, and technical control measures for the proposed property management system. There are several layers of security that FHA will need to address after the ASP is selected and more technical details become available. They are:

- Network Security.
- Operating System Security.
- Database Server Security.
- Application Security.

FHA, in conjunction with the ASP, will need to update the *System Security and Privacy Plan* to define management, operational, and technical controls for each of the security layers, where appropriate.

3.1.1 Management Controls

Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management. To assess management controls, FHA will review:

- Risk management.
- Security control reviews.
- Life cycle plans.
- Authorize processing – certification and accreditation.

3.1.1.1 Risk Management

During the Initiate phase, FHA completed the *Risk Analysis* SDM document. The *Risk Analysis* documents the initial risk assessment for the proposed property management system and an approach for conducting future risk assessments. It identifies the project management structure, risk management structure, and schedule for periodic risk assessments. The *Risk Analysis* also:

- Presents some physical, management, hardware, and software risks associated with the proposed system.
- Determines the necessary safeguards to mitigate the risks to the proposed system.
- Evaluates the identified safeguards for cost and economic feasibility.

In the future, FHA will perform a quantifiable risk assessment and will develop management controls to establish organization, policies, and procedures. The outcomes of the quantifiable risk assessment will drive the development of planned security controls and countermeasures to ensure risks are mitigated to an acceptable level. FHA will also conduct a mission/business impact analysis and develop an organization chart of the project team, subject matter experts related to the project, and key stakeholders.

In addition, FHA will establish a Quality Assurance team to review all documents for consistency and adherence to HUD's SDM. This team will work with the functional, technical, and change management teams to verify that all project deliverables and work products follow legislation and regulations. This team will work with project management to assure that the program achieves its intended results and that the programs and resources are protected from waste, fraud, and mismanagement.

3.1.1.2 Security Control Reviews

Routine evaluations and response to identified vulnerabilities are important elements of managing the risk of a system. The project team will be responsible for establishing periodic reviews of the security controls for the new property management system and each of its interconnected systems. The reviews may include routine self-assessments, independent reviews after significant changes occur, network scans for vulnerable software and network services, reviews of router and firewall configurations, and external penetration testing. The project team will also be responsible for establishing an effective and timely process for reporting significant weaknesses and ensuring effective remedial action.

3.1.1.3 Life Cycle Plans

Planning for system security is a continuous process, conducted throughout the lifecycle of a system. FHA will update this document during each phase of HUD's SDM – Initiate, Development and Acquisition, Implement, Operational and Maintenance, and Disposal - to

accurately reflect changes and new information. This section of the document describes each phase of the SDM as the project progresses.

- **Initiate phase** – During the Initiate phase, the need for a system is expressed and the purpose of the system is documented. FHA is currently in the Initiate phase of HUD's SDM. To support this effort, FHA completed the *Risk Analysis* report, which documents the initial risk assessment for the proposed property management system and an approach for conducting future risk assessments. It identifies the project management structure, risk management structure, and schedule for periodic risk assessments. FHA also drafted this *System Security and Privacy Plan*, which assesses the sensitivity of the information contained within the new system and the risk level for confidentiality, integrity, and availability as well as addresses the measures necessary for system security.
- **Development and Acquisition phase** – During this phase, the system requirements are defined, the ASP is selected, and the contract is negotiated. FHA will develop the security requirements in conjunction with the functional and technical requirements of the system. FHA will need to define its procedures for security operations and administration, operational assurance, and auditing and monitoring within the *System Security Plan*. In an ASP environment, the *System Security Plan* is an important management control. These requirements will be used to support the selection and contract negotiation process.
- **Implementation phase** – During this phase, the system is implemented and tested. In conjunction with the ASP, FHA will configure and enable the system's security features, test the system, and authorize the system processing. If new controls are added, additional acceptance testing must be performed. The results of the reviews and tests need to be documented, updated, and maintained.
- **Operational and Maintenance phase** – During this phase, the system performs its work. The ASP will perform the required security activities as outlined in their contract and the *System Security Plan*. FHA will perform the security oversight activities outlined in the *System Security Plan*.
- **Disposal phase** The disposal phase involves the disposition or archival of information, hardware, and software. In conjunction with the ASP, FHA will need to define its archival process during the development and acquisition phase.

3.1.1.4 Authorize Processing – Certification and Accreditation.

Accreditation is the authorization granted by a management official for a system to process information. Authorize processing provides a form of assurance of the security of the system. It requires managers and technical staff to identify the best approach to security management and risk mitigation given current or future constraints. When a manager authorizes processing of a system, the manager accepts the risks associated with system.

In order for the new property management system to be granted authorization to process information, the project team will need to accomplish a series of system security tasks. To date, FHA has conducted an initial risk assessment, as documented in the *Risk Analysis* report, and has completed this *System Security and Privacy Plan*. In the future, the system security tasks that FHA may need to accomplish include:

- Completing a technical and/or security evaluation.
- Establishing Rules of Behavior for system users.
- Developing and testing a contingency plan.
- Ensuring controls are consistent with identified risks and are operating as intended.
- Determining how often to require re-authorization of processing.

3.1.2 Operational Controls

Operational controls address security methods implemented and executed by people as opposed to systems. These controls are implemented to improve the security of a system or group of systems. With an ASP solution, proper security is largely dependent on other organizations and their security tools and technologies. To assess operational controls, FHA will review:

- Personnel security.
- Physical and environmental protection.
- Production and input/output controls.
- Contingency planning.
- Hardware and software maintenance.
- Data integrity.
- Documentation.
- Security awareness, training, and education.
- Incidence response capability.

3.1.2.1 Personnel Security

Personnel security relates to how users, designers, implementers, and managers interact with systems and the access and authorities that they need to do their jobs. FHA will maintain proper segregation of duties to ensure the least privilege and individual accountability. FHA will also need to perform background screenings prior to granting users access to the system. Other security requirements may include:

- Reviewing all positions for sensitivity level.
- Dividing sensitive functions among different individuals.
- Implementing mechanisms to hold users responsible for their actions.
- Establishing processes for requesting, establishing, issuing, and closing user accounts.

3.1.2.2 Physical and Environmental Protection

Physical security and environmental security are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment.

FHA will ensure that HUD and the ASP facilities have adequate physical security controls commensurate with risks of physical damage or access. This may include physical access controls or biometrics and environmental planning. Physical access controls restrict the entry and exit of personnel, equipment, and media from a specified area through the use of guards, identification badges, key cards, motion sensors, or other mechanisms. Biometrics and environmental planning protect against fire or failure of supporting utilities, such as failures of electric power, heating and air-conditioning systems, water, sewage, and other utilities that may interrupt services or damage hardware. In addition, FHA will ensure data is protected from interception through securing physical access to data transmission lines. Other security controls may involve:

- Conducting management reviews on the list of persons with physical access to sensitive facilities.
- Changing entry codes periodically.
- Monitoring physical accesses through audit trails.
- Investigating apparent security violations.
- Providing an uninterruptible power supply or backup generator.

FHA has developed the *Risk Analysis* document, which includes a discussion of physical and environmental protection as well as emergency planning. FHA will coordinate the implementation of these controls with HUD Automated Data Processing (ADP) Security group to improve the security of the property management system and the ASP site.

3.1.2.3 Production and Input/Output Controls

Production and input/output controls pertain to user support and procedures for protecting media. As part of the contract with the ASP, the ASP will provide help desk support for users. FHA will ensure that there are adequate procedures in place for storing, handling, and destroying media. Other security requirements may involve:

- Using audit trails for receipt of sensitive inputs/outputs.
- Shredding or destroying hardcopy media when no longer needed.

3.1.2.4 Contingency Planning

Contingency planning addresses how to keep an organization's critical functions operating in the event of disruptions, large or small. FHA has a disaster recovery plan in place for current property disposition systems and supporting operations. FHA will work with the ASP to develop a comprehensive contingency plan once the contract is awarded. For the new system, FHA will work with the ASP to:

- Identify the most critical and sensitive operations and their supporting computer and personnel resources.
- Define recovery requirements and timeframes to ensure a balance between cost effectiveness and risk mitigation.
- Develop and document a comprehensive contingency plan.
- Test the contingency/disaster recovery plan.

3.1.2.5 Hardware and Software Maintenance

These are controls used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes. These controls include implementing restrictions on access to system software and hardware as well as authorizing, testing, and approving all new software and hardware before implementation. FHA will develop the *Configuration Management Plan* to define the maintenance and control of application software and documentation. Parallel to the management of application changes is proper management of changes to the supporting infrastructure, such as servers, their operating systems and databases, and other network devices. These devices play a critical role in the successful operation of FHA's future application and must be constantly monitored and updated for security patches. These day-to-day procedures and mechanisms will be used to protect system software and hardware.

3.1.2.6 Data Integrity

Data integrity controls are used to protect data from accidental or malicious alteration or destruction. These controls also provide assurance to the user that the information meets expectations about its quality and integrity. FHA will ensure the ASP installs, activates, and routinely updates virus detection and elimination software. Data integrity and validation controls will be used to provide assurance that the information has not been altered and the system functions as intended. Other security requirements may involve:

- Implementing procedures to ensure compliance with password policies.
- Installing intrusion detection tools on the system.
- Performing external penetration testing on the system.

3.1.2.7 Documentation

Documentation is a control that describes the hardware, software, policies, standards, procedures, and approvals related to the system and formalizes the system's security controls. The ASP will provide user manuals as well as documentation for all software and hardware. The ASP will also provide documentation for testing, emergency, and backup procedures. It is FHA's responsibility to ensure that formal security and operational procedures are documented. The project team will also be responsible for ensuring that all necessary SDM documents are completed. Security documentation may also include:

- Risk assessment reports.
- Contingency plan.

3.1.2.8 Security Awareness, Training, and Education

Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge. *OMB Circular A-130, Management of Federal Information Resources, Appendix III*, requires the establishment of application specific rules and communication of these rules before system access is allowed. Failure to do so constitutes an automatic deficiency under *OMB Circular A-123* and *OMB Circular A-130*. All employees and contractors involved with the management, use, design, development, maintenance or operation of the application should be aware of the system rules and their responsibilities prior to access. Appropriate background checks will be conducted for all contractors and FHA users prior to gaining access to the system.

Training will include application user, administrator, and introductory awareness and security-related training. Each user will be versed in acceptable rules of behavior for the application. During end-user training, users will be informed about the procedures for reporting security incidents.

3.1.2.9 Incidence Response Capability

Computer security incidents are an adverse event in a computer system or network. The ASP will provide help to users when a security incident occurs in the system. This may involve developing a formal incident response capability, monitoring incidents until resolved, and training staff to handle incidents. FHA and the ASP will work together to ensure incident-related information is shared with the appropriate organizations.

An important aspect of incident response is detection and prevention. Not all security and network risks can be mitigated; therefore, the ability to detect network probes and attacks is critical to maintaining the availability, confidentiality, and integrity of the proposed system. The ASP must have a mature incidence response capability and a deployed Intrusion Detection System (IDS). This latter point has been mandated by Congress under the Federal Information Security Requirements Act (FISMA), which also requires Federal agencies to report annually to OMB on their incident response capabilities.

Prevention is a critical activity in maintaining the security of a future system. The Federal government has issued formal guidance under NIST *Special Publication 800-40 Procedures for Handling Security Patches*. CERT/ Coordination Center estimates that 95 percent of all network intrusions could be avoided by keeping systems up to date with appropriate patches.[1] Therefore, the future ASP must demonstrate a mature process for deploying security patches in a timely manner to ensure FHA's application and supporting infrastructure are adequately protected.

[1] Note: CERT is no longer an acronym. Previously it stood for Computer Emergency Response Team. Please see http://www.cert.org for more information.

3.1.3 Technical Controls

Technical controls focus on security controls that the computer system executes. The technical controls focus on processes for confidentiality and data integrity. The controls will provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. To assess technical controls, FHA will review:

- Identification and authentication.
- Logical access controls.
- Audit trails.

3.1.3.1 Identification and Authentication

Identification and authentication is a technical measure that prevents unauthorized people from entering an IT system. The new property management system will have access controls that will identify, differentiate, and authenticate users via passwords, tokens, or other devices. The preferred method of authentication requires the use of digital certificates that provide the element of technical non-repudiation. Use of digital certificates and mutual authentication (client to server, server to client) assures users are properly authenticated and their identity is clearly established. The system will also use role-based access controls to enforce segregation of duties.

FHA will develop an application role user matrix to define user identification, correlation of actions to users, maintenance of user ids and user lists, identification and authentication, and logical access controls. The matrix will define users with direct access to the system and those who will indirectly receive output from the system. The matrix will also include the levels of security investigation and system access required for each user. FHA will work with the ASP to ensure the property management system maintains accurate access levels for each user.

Other security requirements may include:

- Prohibiting access scripts with embedded passwords.
- Limiting invalid access attempts for a given user.
- Implementing procedures for handling lost and compromised passwords.

3.1.3.2 Logical Access Controls

Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. The new property management system will use logical access controls to restrict users to authorized transactions and functions. The system will also use logic controls, such as firewalls and monitored access, to protect network access. Other security requirements may include:

- Restricting access to security software to security administrators.
- Monitoring access to the system and network to identify apparent security violations and investigating such events.
- Restricting access to tables defining network options, resources, and operator profiles.

3.1.3.3 Audit Trails

Audit trails maintain a record of activity by system or application processes and by user activity. The new property management system will include audit functionality over login attempts to detect misuse and misbehavior. Furthermore, the new system must maintain records of approval and authorization of individual transactions and may store the “before picture” of changed data. Anti-virus software will detect potentially malicious code on the client and an IDS will detect attempted attacks and network probes by unauthorized persons. System administrators will also review control and audit logs from servers, firewalls, and routers to assess penetration attempts or network anomalies. Other security requirements may include:

- Maintaining audit trails of logons to network, operating system, database, and application.
- Conducting correlation analysis on IDS sensors to firewall and application logs.

3.2 System Security

Using federal and regulatory statutes, FHA will develop the necessary blueprint for the overall organizational security model. In the ASP solution, FHA partners with the service provider to configure the system to meet the business and technical needs. This partnership also addresses the security plan. The security burden crosses three areas:

- FHA responsibilities.
- ASP responsibilities.
- Shared responsibilities.

FHA will develop the materials for the user training and can stress the importance of both physical (papers on desk, writing passwords on post-it notes, logoff screens after specific time of inactivity, day-to-day user procedures) and system security (user passwords and IDs are current, strong password policies.) As the ASP hosts the database and application, security for both resides with the ASP. FHA will ensure that the selected ASP conforms to federal security mandates and legislation. The ASP will provide redundant and/or fault-tolerant systems and will provide a business continuity plan based on HUD’s current policies.

Network security may fall under a shared responsibility. Network security is partially determined by “ownership” of the network. For example, HUD’s network is controlled and secured by HUD or its contractors. However, the ASP may control security over the Internet and access to the application and database.

FHA needs to clearly define roles and responsibilities for the network prior to negotiations and use these requirements to solidify the contract. FHA will continue to define security requirements in subsequent project phases.